SPRINGER'S REGULAR ELEMENTS OVER ARBITRARY FIELDS

V. REINER, D. STANTON, AND P. WEBB

Abstract. Springer's theory of regular elements in complex reflection groups is generalized to arbitrary fields. Consequences for the *cyclic sieving phenomenon* in combinatorics are discussed.

1. Introduction

This paper generalizes Springer's theory of regular elements in complex reflection groups, extending it to reflection groups over an arbitrary field whose polynomial invariants form a polynomial algebra. We begin by discussing Springer's results, and some of our motivation.

An element g in $GL_n(\mathbb{C})$ of finite order is called a *reflection* if its fixed subspace in $\mathbb{C}^n$ is a hyperplane (codimension 1 linear subspace), called the *reflecting hyperplane* for g. A finite subgroup G of $GL_n(\mathbb{C})$ is called a *complex reflection group* if it is generated by reflections. Shephard and Todd [17] classified such groups. They used this classification to prove that they are exactly the groups G whose action on the polynomial ring $S := \mathbb{C}[x_1, \ldots, x_n]$ has invariants $S^G = \mathbb{C}[f_1, \ldots, f_n]$ which form a polynomial algebra. This was re-proven in a uniform fashion by Chevalley [5]. Chevalley also used the Normal Basis Theorem of Galois Theory to prove a fact about the induced G-action on the *coinvariant algebra*

$$A := S/(f_1, \ldots, f_n) = S \otimes_{S^G} \mathbb{C}.$$

Here $\mathbb{C}$ is considered as the trivial S^G-module $\mathbb{C} := S^G/S^G_+$, where S^G_+ is the set of elements of positive degree in S^G. His result says that the coinvariant algebra A is isomorphic to the regular representation $\mathbb{C}[G]$ as a (ungraded) $\mathbb{C}[G]$-module.

Springer generalized this isomorphism to incorporate a larger group action. Say that a vector v in $\mathbb{C}^n$ is *regular* if it lies on none of the reflecting hyperplanes for reflections in G, and say that an element c in G is regular if it has a regular eigenvector v, say with eigenvalue $\omega \in \mathbb{C}^\times$. The cyclic group $C = \langle c \rangle$ generated by a regular element c acts on S and on the coinvariant algebra A by the *scalar* substitution $c(x_i) = \omega x_i$ for all i. Note that this C-action is distinct from the action by linear substitutions which C inherits as a subgroup of G. In fact, the C-action by scalar substitutions commutes with the G-action, making A into a $\mathbb{C}[G \times C]$-module. There is also a natural $\mathbb{C}[G \times C]$-module structure on the group algebra $\mathbb{C}[G]$, in which G multiplies on the left and C multiplies on the right. One

Date: November 2004.

1991 *Mathematics Subject Classification.* 13A50, 51F15, 20F55.

Key words and phrases. Dickson invariants, coinvariant algebra, reflection group, Springer regular element, Kraśkiewicz-Weyman, Singer cycle, cyclic sieving phenomenon.

First, second author supported by NSF grants DMS-0245379, DMS-0203282 respectively.

of Springer's main results can be rephrased (following Kraskiewicz and Weyman [11]; see also [20]) as follows.

Theorem (Springer [19]). *The coinvariant algebra A and the group algebra $\mathbb{C}[G]$ are isomorphic as (ungraded) $\mathbb{C}[G \times C]$-modules.*

Our goal is to extend this result to fields other than $\mathbb{C}$. Let V be an n-dimensional vector space over an arbitrary field k and G a finite subgroup of $GL(V)$. Let S denote the symmetric algebra of V^*, so that we may identify $S = k[x_1, \ldots, x_n]$ by choosing a basis $x_1, \ldots, x_n$ for V^*. In this context, define a *reflection* to be an element of $GL(V)$ of finite order whose fixed subspace is a hyperplane (it is not assumed that a reflection is semisimple). Our starting point is a result of Serre [16] that generalizes half of the Shephard-Todd and Chevalley result: if the invariant ring S^G is a polynomial algebra $k[f_1, \ldots, f_n]$, then G must be generated by reflections. Mitchell [12] proved a result generalizing that of Chevalley in this context: the coinvariant algebra

$$A := S/(f_1, \ldots, f_n) = S \otimes_{S^G} k$$

and the regular representation $k[G]$ have the same composition factors as $k[G]$-modules.

Given such a reflection group G, define regular vectors and regular elements as follows. Let $\bar{k}$ be the algebraic closure of k, let $\overline{V} := V \otimes_k \bar{k}$, and $\bar{S} := S \otimes_k \bar{k} \cong \bar{k}[x_1, \ldots, x_n]$. Say that a vector $v \in \overline{V}$ is *regular* if it lies on none of the reflecting hyperplanes $\bar{H} := H \otimes_k \bar{k}$ for reflections in G, that is, if v is not fixed by any reflection in G. Define c in G to be *regular* if it has a regular eigenvector $v \in \overline{V}$, say with eigenvalue $\zeta \in \bar{k}^\times$. It will be seen below (Corollary 7) that this implies c is also *p-regular*, that is, its multiplicative order is invertible in the field k. Consequently c acts semisimply on V and in any other representation of G over k.

If $C := \langle c \rangle$, then as before, both the coinvariant algebra (with scalars extended to $\bar{k}$)

$$\bar{A} := \bar{S}/(f_1, \ldots, f_n) = \bar{S} \otimes_{\bar{S}^G} \bar{k}$$

and the group algebra $\bar{k}[G]$ can be made into $\bar{k}[G \times C]$-modules:

- G acts on $\bar{A}$ by linear substitutions, and C acts on $\bar{A}$ by the scalar substitution $c(x_i) = \zeta x_i$ for all i, while
- G multiplies $\bar{k}[G]$ on the left and C multiplies it on the right.

We comment that for general subgroups C, in order to make $\bar{k}[G]$ into a left $\bar{k}[G \times C]$-module an element $c \in C$ must multiply on the right by c^{-1}. However, since C is abelian and inversion is a group automorphism, we do not need to introduce an inverse to obtain a group action, and since $\bar{k}[G]$ is a permutation representation for C, whether we introduce an inverse or not we obtain isomorphic results.

Theorem 1. *Let V be a finite-dimensional vector space over an arbitrary field k. Let G be a finite subgroup of $GL(V)$ for which S^G is polynomial. Then the coinvariant algebra $\bar{A}$ and the group algebra $\bar{k}[G]$ have the same composition factors as $\bar{k}[G \times C]$-modules,*

Theorem 1 generalizes a previous result of the authors [13, Theorem 1] where $G = GL_n(\mathbb{F}_q)$. The proof of Theorem 1 follows the same outline as Springer's, with a few complications due to the field being arbitrary. In Section 3 we review Serre's result and some consequences for the reflection groups whose invariants are polynomial.

Section 4 uses this to generalize the crucial facts about regular elements to arbitrary fields, and in Section 5 these facts are assembled into a proof of Theorem 1 via a (Brauer) character computation.

Section 2 discusses one of our main motivations, coming from the *cyclic sieving phenomenon* in combinatorics. Springer's Theorem (over $\mathbb{C}$) immediately implies that for any subgroup H of a complex reflection group G the H-fixed subspaces A^H and $\mathbb{C}[G]^H$ are isomorphic as C-representations. This has combinatorial consequences (see [14]), for which we sought a version valid over all fields. Theorem 2, the other main result of this paper, gives a version valid under some hypotheses on the subgroup H. We also speculate there (Conjecture 3, Question 4) on more general versions.

Section 7 discusses regular elements and examples where $G = GL_n(\mathbb{F}_q)$. Regular elements in this situation are shown to be exactly the elements in the images of the embeddings $\mathbb{F}_{q^n}^\times \hookrightarrow GL_n(\mathbb{F}_q)$ that arise from identifying $\mathbb{F}_{q^n} \cong (\mathbb{F}_q)^n$. Two interesting examples of subgroups H in $GL_n(\mathbb{F}_q)$ are also discussed, one illustrating Theorem 2 when H is the group of *monomial matrices*, the other providing evidence for Conjecture 3 by checking it holds when H is the *symplectic group* $Sp_{2n}(\mathbb{F}_q)$ for q odd.

Section 8 discusses a consequence (Proposition 22) of Theorem 1 relating to "sieving" the composition factors of the group algebra $k[G]$ when k has positive characteristic. It also speculates on the existence of a stronger version of this phenomenon (Question 23).

Throughout the paper, $k, \bar{k}, V, \overline{V}, S, \bar{S}$ will have the same meaning as in this introduction.

2. Combinatorial motivation: the cyclic sieving phenomenon

One of our motivations was to generalize to other fields an enumerative consequence of Springer's Theorem (over $\mathbb{C}$), called the cyclic sieving phenomenon, which we now explain.

Whenever C is a finite cyclic group, X is a finite C-set and $X(t)$ is a polynomial with integer coefficients, we will say that the triple $(X, X(t), C)$ exhibits the *cyclic sieving phenomenon* if either of the following two equivalent conditions (see [14, §2]) holds:

(i) for all $c \in C$ and any $\omega \in \mathbb{C}^\times$ having the same multiplicative order as c, one has
$$|\{x \in X : c(x) = x\}| = [X(t)]_{t=\omega},$$
or

(ii) in the expansion
$$X(t) \equiv \sum_{\ell=0}^{|C|-1} a_\ell t^\ell \mod t^{|C|} - 1,$$
the coefficient a_ℓ counts the number of C-orbits on X in which the C-stabilizer of an element has order dividing ℓ.

One can interpret the special case of condition (i) asserting $|X| = X(1)$ as saying that $X(t)$ is a *generating function* for the set X. In combinatorics, these generating functions $X(t)$ often already have a combinatorial interpretation when t is specialized to a prime power q, enumerating objects associated with the finite field $\mathbb{F}_q$; it

is a pleasant surprise to also have an interpretation when t is a root of unity. See [14] for many instances of this phenomenon, and further motivation.

It is an elementary exercise to show that if the complex characters of C are labelled $\chi_0, \chi_1, \ldots, \chi_{|C|-1}$, in such a way that for $c \in C$ we have $\chi_\ell(c) = \chi_1(c)^\ell$, then the conditions (i) or (ii) say that a_ℓ is the multiplicity of χ_ℓ in the permutation module $\mathbb{C}[X]$, and so $\mathbb{C}[X]$ has character $\sum_\ell a_\ell \chi_\ell$ (see [14, Prop. 2.1]). Thus if we have a graded C-representation

$$A_X = \bigoplus_{i \geq 0} A_{X,i}$$

in which each $c \in C$ acts on $A_{X,i}$ by the scalar $\chi_i(c)$ and we put

$$X(t) = \mathrm{Hilb}(A_X, t) := \sum_{i \geq 0} \dim_{\mathbb{C}} A_{X,i} t^i,$$

then $(X, X(t), C)$ exhibits the cyclic sieving phenomenon if and only if

$$\mathbb{C}[X] \cong A_X \tag{2.1}$$

are isomorphic as C-representations.

The comments just made allow us to construct in abstract a triple which exhibits the cyclic sieving phenomenon starting from any finite C-set X. For applications it is important that such triples should arise in some natural way allowing an interpretation, invariant theory and Springer's Theorem provide such triples whenever whenever X has a transitive action of some group G whose invariant ring S^G is polynomial. In such a situation case, let H be the stabilizer in G of some particular element of X, so that one can identify $X = G/H$. Then one has an isomorphism[1] of C-representations

$$\mathbb{C}[X] = \mathbb{C}[G/H] \cong \mathbb{C}[G]^H. \tag{2.2}$$

On the other hand, Springer's Theorem tells us that the coinvariant algebra A is isomorphic to $\mathbb{C}[G]$ as $G \times C$-representations. Restricting this isomorphism to the H-fixed subspaces gives

$$\mathbb{C}[G]^H \cong A^H, \tag{2.3}$$

and the C-action on A (and hence on A^H) was defined so that A^H can play the role of the graded C-representation A_X above. Hence stringing together (2.2) and (2.3) yields an isomorphism as in (2.1).

Our second main result, Theorem 2 gives a version of this valid for arbitrary fields. Let $V, \overline{V}, k, \bar{k}, S, \bar{S}$ have the same meaning as in the discussion preceding Theorem 1, and let G be a finite subgroup of $GL(V)$ for which S^G is a polynomial algebra. For any subgroup H, define $X := G/H$ and

$$X(t) := \frac{\mathrm{Hilb}(S^H, t)}{\mathrm{Hilb}(S^G, t)} \qquad \left(= \frac{\mathrm{Hilb}(\bar{S}^H, t)}{\mathrm{Hilb}(\bar{S}^G, t)} \right). \tag{2.4}$$

[1]One should be careful about the left and right actions of the (abelian) group C in this isomorphism. On G/H one has C acting by left multiplication, while on $\mathbb{C}[G]^H$ (as on $\mathbb{C}[G]$) one has C acting by right multiplication. The isomorphism $\mathbb{C}[G]^H \cong \mathbb{C}[G/H]$ then maps $(\sum_{h \in H} h)g \mapsto g^{-1}H$.

Provided S^H is a free S^G-module (that is, S^H is *Cohen-Macaulay*), one has the interpretation $X(t) = \mathrm{Hilb}(S^H \otimes_{S^G} k, t)$, so that with this extra hypothesis $X(t)$ is a polynomial with nonnegative integer coefficients. (As will be explained later, $X(t)$ is always polynomial with integer coefficients). In case $|H|$ is invertible in k, one can show furthermore that $X(t) = \mathrm{Hilb}(A^H, t)$.

Theorem 2. *Let V be a finite-dimensional vector space over an arbitrary field k. Let G be a finite subgroup of $GL(V)$ for which S^G is polynomial, and let C be the cyclic subgroup generated by a regular element in G.*

Then under either of the following two conditions on the subgroup H, the triple $(X, X(t), C)$ exhibits the cyclic sieving phenomenon:

Case (a)*: the order $|H|$ is invertible in k, or*
Case (b)*: the invariant subring S^H is also a polynomial algebra.*

Equivalently, since C acts semisimply by Corollary 7, in either Case (a) or (b) above, the C-representations $\bar{S}^H \otimes_{\bar{S}^G} \bar{k}$ and $\bar{k}[G/H]$ are isomorphic.

It is also worth pointing out a very explicit rephrasing of Case (b). Let $H \subset G$ be subgroups of $GL(V)$ with both S^H, S^G polynomial, and let c in G be a regular element of order d. Suppose

$$S^G = k[g_1, \ldots, g_n], \text{ with } \deg(g_i) = d_i^G, \text{ and } a_G(d) := |\{i : d | d_i^G\}|$$
$$S^H = k[h_1, \ldots, h_n], \text{ with } \deg(h_i) = d_i^H \text{ and } a_H(d) := |\{i : d | d_i^H\}|.$$

Theorem 2 Case (b) (rephrased). *Let V be a finite-dimensional vector space over an arbitrary field k. Let $H \subset G$ be subgroups of $GL(V)$ with both S^H, S^G polynomial, and notation as above. Let c be a regular element in G of order d, and ω in $\mathbb{C}^\times$ a primitive d^{th} root of unity.*

Then there are no cosets gH fixed under left-translation by c unless $a_H(d) = a_G(d)$, in which case

$$|\{gH : cgH = gH\}| = \lim_{t \to \omega} \prod_{i=1}^{n} \frac{1 - t^{d_i^G}}{1 - t^{d_i^H}} = \frac{\prod_{i:d|d_i^G} d_i^G}{\prod_{i:d|d_i^H} d_i^H} \tag{2.5}$$

Theorem 2 is an immediate consequence of Theorem 1 in Case (a), but not (as far as we are aware) in Case (b). Section 6 gives a proof using facts about regular elements. This generalizes the special case where $G = GL_n(\mathbb{F}_q)$ and H is a *parabolic subgroup* that appeared as [13, Theorem 2].

Conjecture 3. *The conclusion of Theorem 2 holds under the weaker hypothesis that S^H is Cohen-Macaulay.*

We have been led to consider these questions when H is an arbitrary subgroup of a group G for which S^G is polynomial, not just one for which S^H is Cohen-Macaulay. We point out that in general $X(t)$ has the following interpretation. Since S^G is a polynomial algebra, the Hilbert Syzygy Theorem implies that S^H has a (graded) finite free resolution as a (graded) S^G-module

$$0 \to \bigoplus_j S^G(-j)^{\beta_{h,j}} \to \cdots \to \bigoplus_j S^G(-j)^{\beta_{0,j}} \to S^H \to 0,$$

where here $S^G(-j)$ denotes a free S^G-module of rank one whose basis element has degree j. Hence $X(t) = \sum_{i,j \geq 0} (-1)^i \beta_{i,j} t^j$, and this is always a polynomial in t with integer coefficients.

Question 4. Does the same conclusion hold (i.e. the cyclic sieving phenomenon for $(X, X(t), C)$ where $X = G/H$ and $X(t)$ is defined as in (2.4)) without *any* hypotheses on the subgroup H?

An affirmative answer to Question 4 would have useful consequences. Firstly, it would provide many more examples of the cyclic sieving phenomenon in combinatorics. Secondly, it is well-known that the general linear group $G = GL_n(\mathbb{F}_q)$ has S^G polynomial (see Section 7). Therefore, whenever H is a subgroup of $G = GL_n(\mathbb{F}_q)$ for which Question 4 has an affirmative answer, version (ii) of the cyclic sieving phenomenon gives a constraint on $\mathrm{Hilb}(S^H, t)$ that can save time in its computation.

3. Serre's result and some consequences

We begin by recalling a fundamental result of Serre.

Theorem 5. *(Serre* [16]*; see also Bourbaki* [3, Chap. V, §5, Exer. 7,8]*) Let G be a finite subgroup of $GL(V)$ for which S^G is a polynomial algebra. Then*

(i) *G is generated by reflections, and*
(ii) *for every k-subspace V' of V, the pointwise stabilizer*

$$G_{V'} := \{g \in G : g|_{V'} = 1_{V'}\}$$

also has $S^{G_{V'}}$ polynomial (and hence $G_{V'}$ is generated by reflections).

This has the following consequence, generalizing [19, Proposition 4.1 (i)]. Although straightforward, we include the proof because it may be not be completely obvious, due to the fact that Serre's result refers to k-subspaces, not $\bar{k}$-subspaces. For a vector v in V, let G_v denote the pointwise stabilizer of the 1-dimensional subspace spanned by v.

Corollary 6. *A vector $v \in \overline{V}$ avoids all the reflecting hyperplanes for G if and only if G acts freely on its orbit, i.e. its pointwise stabilizer $G_v = 1$.*

Proof. Assume v avoids all the reflecting hyperplanes for G. Consider the k-subspace

$$V' = \bigcap_{g \in G_v} \ker(g - 1_V) = \ker\left(V \xrightarrow{\oplus_{g \in G_v} g-1} \bigoplus_{g \in G_v} V \right).$$

Then v lies in its extension by scalars

$$\bar{V}' := V' \otimes_k \bar{k} = \bigcap_{g \in G_v} \ker(g - 1_{\overline{V}}) = \ker\left(\overline{V} \xrightarrow{\oplus_{g \in G_v} g-1} \bigoplus_{g \in G_v} \overline{V} \right).$$

Furthermore, $G_v \subset G_{V'}$, so it suffices for us to show that $G_{V'} = 1$. By Serre's Theorem, $G_{V'}$ is generated by reflections r in G, which must necessarily all satisfy $V' \subset \ker(r - 1_V)$. But then $v \in \bar{V}' \subset \ker(r - 1_{\overline{V}})$, i.e. r fixes v. Since v avoids all the hyperplanes for G, there are no such reflections, and $G_{V'} = 1$. □

This last corollary has another important consequence mentioned in the Introduction.

Corollary 7. *Let G be a finite subgroup of $GL(V)$ for which S^G is polynomial, and c a regular element. Then c is p-regular, that is, its multiplicative order is invertible in k. In particular, c acts semisimply on V.*

Proof. Let v be a regular eigenvector for c with corresponding eigenvalue ζ in $\bar{k}$. Let c, ζ have multiplicative orders d, d', respectively, so that d' divides d. We claim that $d = d'$. To see this, note that

$$c^{d'}(v) = \zeta^{d'} \cdot v = v$$

and hence $c^{d'}$ lies in the pointwise stabilizer G_v. As $G_v = 1$ by Corollary 6, one has $c^{d'} = 1$, so d divides d', and hence $d = d'$.

But d' is invertible in k. To see this, observe that if k has characteristic $p > 0$, then ζ being of finite order implies that it generates a finite extension $\mathbb{F}_p(\zeta)$ of the prime field. If $|\mathbb{F}_p(\zeta)| = p^r$, then ζ has its order d' dividing $|\mathbb{F}_p(\zeta)^\times| = p^r - 1$, and hence is coprime to p. □

In working over $\mathbb{C}$, Springer's methods use in a crucial way a classical fact about the *Jacobian determinant*

$$J = \det\left(\frac{\partial f_i}{\partial x_j}\right)$$

where $S^G = k[f_1, \ldots, f_n]$ for homogeneous invariants $f_1, \ldots, f_n$. For complex reflection groups there is a well-known factorization of J into products of powers of the linear forms that define the reflecting hyperplanes for G. This implies that the zero set for J in $\mathbb{C}^n$ is the union of the reflecting hyperplanes of G, and the same is known to hold more generally when k has characteristic zero.

A more general result holds over arbitrary fields, and is crucial for the sequel. The authors thank W. Messing for providing a proof of the following generalization, using results of Grothendieck on étale coverings.

Theorem 8. *When $S^G = k[f_1, \ldots, f_n]$ is a polynomial algebra, the zero set of the Jacobian J in V (or $\overline{V}$) is the union of the reflecting hyperplanes for G.*

Proof. The inclusion of rings $\bar{S}^G \hookrightarrow \bar{S}$ corresponds to the quotient map $\overline{V} \stackrel{\pi}{\twoheadrightarrow} \overline{V}/G$. Because the field extension

$$\mathrm{Frac}(\bar{S}^G) = \mathrm{Frac}(\bar{S})^G \hookrightarrow \mathrm{Frac}(\bar{S})$$

is separable of degree $|G|$, the map π is a separated morphism of schemes which is quasifinite of degree $|G|$. Therefore [15, Exposé I, §10, Théorème 10.11] says that there is a neighborhood of v in V in which π is an étale covering if and only if the fiber $\pi^{-1}(\pi(v))$ has exactly $|G|$ preimages. By Corollary 6, the latter condition occurs if and only if v lies on none of the reflecting hyperplanes of G.

On the other hand, since $\overline{V}$ and $\overline{V}/G$ are both smooth schemes (the latter because $\bar{S}^G$ is polynomial), one can apply [15, Exposé II, §4, Corollaire 4.6] to assert that π is étale in a neighborhood of v in V if and only if the mapping of cotangent spaces

$$\Omega^1(\overline{V}/G)_{\pi(v)} \xrightarrow{\pi^*} \Omega^1(\overline{V})_v$$

is an isomorphism. As this mapping is represented in coordinates by the Jacobian matrix $\left(\frac{\partial f_i}{\partial x_j}(v)\right)_{i,j=1,\ldots,n}$ evaluated at v, it will be an isomorphism if and only if $J(v) \neq 0$. The theorem follows. □

Remark 9. The above theorem also follows from a recent (independent) result of Hartmann and Shepler [8], who give an explicit factorization of J into products of powers of the linear forms ℓ_H defining the reflecting hyperplanes H. Given such a hyperplane H, recall that G_H denotes its pointwise stabilizer, and Theorem 5

implies that S^{G_H} is also a polynomial algebra. Let d_H denote the sum of the degrees $d_1, \ldots, d_n$ for any n basic (homogeneous) invariants which generate S^{G_H} . Hartmann and Shepler show that, up to a constant in $k^\times$,

$$J = \prod_H \ell_H^{d_H - n}$$

where the product runs through all reflecting hyperplanes H for G.

4. Regular elements

This section generalizes facts on regular elements in reflection groups over the complex numbers to arbitrary fields. These facts are necessary for the proof of Theorem 1.

For the remainder of this section, we assume that $S^G = k[f_1, \ldots, f_n]$ is a polynomial algebra, with f_i homogeneous of degree d_i. For a positive integer d, let

$$a(d) := |\{i : d | d_i\}|.$$

For g in G and $\zeta \in \bar{k}$, let $\overline{V}(g, \zeta)$ be the ζ-eigenspace for g acting on $\overline{V}$. For a polynomial $f \in S$ (or $\bar{S}$), let $Z_{\bar{k}}(f)$ denote the zero locus of f in $\overline{V}$.

The following two propositions are proven exactly as in [19, Proposition 3.2, Theorem 3.4]. The important features are that $f_1, \ldots, f_n$ form a regular sequence in S or $\bar{S}$, and that $\bar{k}$ is algebraically closed so that two points v, v' in $\overline{V}$ lie in the same G-orbit if and only if $f_i(v) = f_i(v')$ for $i = 1, 2, \ldots, n$.

Proposition 10. *Let $\zeta \in \bar{k}$ be a primitive d^{th} root of unity. Then*

$$\bigcup_{g \in G} \overline{V}(g, \zeta) = \bigcap_{i : d \nmid d_i} Z_{\bar{k}}(f_i).$$

Furthermore, the irreducible components of this algebraic set are those eigenspaces $\overline{V}(g, \zeta)$ which are maximal under inclusion, and each has dimension $a(d)$.

Proposition 11. *Let $\zeta \in \bar{k}$ be a primitive d^{th} root of unity.*

If $\dim \overline{V}(g, \zeta) = \dim \overline{V}(g', \zeta) = a(d)$, then there exists $h \in G$ with $\overline{V}(g', \zeta) = h(\overline{V}(g, \zeta))$.

The following result is not quite as strong as Springer's [19, Theorem 2.4 (i),(ii)] (for $k = \mathbb{C}$) because of its hypothesis that $f_1, \ldots, f_n$ is a system of parameters, and not just algebraically independent. But it will suffice for our purposes, namely to prove Proposition 14 below.

Lemma 12. *(Smith* [18, Prop. 5.5.5]*) Let G be a finite subgroup of $GL(V)$. Suppose that S^G contains a homogenous system of parameters $f_1, \ldots, f_n$ with degrees $d_1, \ldots, d_n$. Then*

(i) *$|G| \leq d_1 \cdots d_n$, and*
(ii) *if equality holds in (i) then $S^G = k[f_1, \ldots, f_n]$.*

Remark 13. Actually [18, Prop. 5.5.5] only states assertion (ii), but Smith's method of proof shows assertion (i) also. Specifically, one applies his Proposition 5.5.2 to the finite extension $k[f_1, \ldots, f_n] \hookrightarrow S^G$ and reasons using his Theorem 5.5.3.

The next proposition appears (for $k = \mathbb{C}$) as [19, Proposition 3.5] and lies at the heart of Springer's theory. In particular, its assertion (ii) shows that if S^G is polynomial, then elements g having $\dim \overline{V}(g,\zeta)$ as large as possible give rise to a smaller group K acting naturally on $\overline{V}(g,\zeta)$, again with polynomial invariants. For the sake of stating this, we introduce some notation. Assume $g \in G$ achieves $\dim \overline{V}(g,\zeta) = a(d)$. Let

$$\begin{aligned} \mathrm{Stab}_G(\overline{V}(g,\zeta)) &:= \{h \in G : h(\overline{V}(g,\zeta)) = \overline{V}(g,\zeta)\}, \\ G_{\overline{V}(g,\zeta)} &:= \{h \in G : h|_{\overline{V}(g,\zeta)} = 1_{\overline{V}(g,\zeta)}\}, \text{ and} \\ K &:= \mathrm{Stab}_{\overline{V}(g,\zeta)}/G_{\overline{V}(g,\zeta)} \\ \mathrm{Cent}_G(g) &:= \{h \in G : hg = gh\} \end{aligned}$$

Note that here, $\mathrm{Stab}_G(U)$ denotes the not-necessarily-pointwise stabilizer subgroup of a subspace U, as opposed to the pointwise stabilizer subgroup G_U.

Proposition 14. *Assume G is a finite subgroup of $GL(V)$ having S^G a polynomial algebra. Further assume that $\dim \overline{V}(g,\zeta) = a(d)$, and let*

$$\mathrm{Stab}_G(\overline{V}(g,\zeta)),\ G_{\overline{V}(g,\zeta)},\ K,\ \mathrm{Cent}_G(g)$$

be defined as in the previous paragraph. Then

(i) $|K| \leq \prod_{i:d|d_i} d_i$.

(ii) *If $|K| = \prod_{i:d|d_i} d_i$, then the K-invariant subalgebra of $S(\overline{V}(g,\zeta))$ is a polynomial algebra on generators $\{f_i|_{\overline{V}(g,\zeta)} : d|d_i\}$. That is,*

$$S(\overline{V}(g,\zeta))^K = \bar{k}[f_i|_{\overline{V}(g,\zeta)} : d|d_i].$$

(iii) *If $G_{\overline{V}(g,\zeta)} = 1$ (e.g. if g is a regular element having a regular vector in $\overline{V}(g,\zeta)$), then*

$$K \cong \mathrm{Stab}_G(\overline{V}(g,\zeta)) = \mathrm{Cent}_G(g),$$

and all these subgroups have cardinality $\prod_{i:d|d_i} d_i$.

Proof. Same as the proof of [19, Proposition 3.5]. One needs to note, however, that Lemma 12 applies because Springer's argument in the proof of [19, Theorem 3.4 (iii)] shows that $\{f_i|_{\overline{V}(g,\zeta)}\}_{i:d|d_i}$ are not only algebraically independent, but also form a system of parameters in this situation. □

The following result (for $k = \mathbb{C}$) is [19, Theorem 4.2].

Theorem 15. *Assume G is a finite subgroup of $GL(V)$ having S^G a polynomial algebra, with notation as above. Let c in G be a regular element, with regular eigenvector v having eigenvalue $\zeta \in \bar{k}$, a primitive d^{th} root of unity.*

(i) $c^d = 1$.

(ii) $\dim_{\bar{k}} \overline{V}(c,\zeta) = a(d)$.

(iii) *The centralizer of c in G is isomorphic to a reflection group whose degrees of basic invariants are the d_i divisible by d, and whose order is $\prod_{i:d|d_i} d_i$.*

(iv) *The elements g in G satisfying $\dim_{\bar{k}} \overline{V}(g,\zeta) = a(d)$ are all conjugate.*

(v) *The eigenvalues of c are $\{\zeta^{1-d_i}\}_{i=1}^n$.*

Proof. Proven exactly as in [19, Theorem 4.2]. A crucial point in the proof of (v) is the fact that a regular vector v will have $J(v) \neq 0$, which follows from Theorem 8. □

5. Proof of Theorem 1

The proof of Theorem 1 relies on the theory of Brauer characters; see [6, §82]. For a finite group H, a $\bar{k}[H]$-module W, and $h \in H$ a p-regular element (that is, one whose multiplicative order is invertible in $\bar{k}$), let $\phi_W^H(h) \in \mathbb{C}$ denote the Brauer character value of h on W. If $W = \bigoplus_m W_m$ is a graded $\bar{k}[H]$-module, define its *graded Brauer character* by

$$\phi_W^H(h;t) := \sum_m \phi_{W_m}^H(h)\ t^m.$$

To prove the theorem, we must show that for every p-regular element $(g,c) \in G \times C$, there is an equality of the Brauer character values

$$\phi_{\bar{k}[G]}^{G\times C}((g,c)) = \phi_{\bar{A}}^{G\times C}((g,c)). \tag{5.1}$$

We begin by computing the left side of (5.1).

Proposition 16. *Let c be a regular element in G of multiplicative order d, and let g be any element of G. Then*

$$\phi_{\bar{k}[G]}^{G\times C}((g,c)) = \begin{cases} |\mathrm{Cent}_G(c)| = \prod_{i:d|d_i} d_i & \text{if } g^{-1} \text{ is } G\text{-conjugate to } c, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Note that $\bar{k}[G]$ is a permutation representation of $G \times C$ and therefore lifts to a representation defined over $\mathbb{Z}$. Hence its Brauer character is its usual character, namely $\phi_{\bar{k}[G]}^{G\times C}((g,c))$ is the number of points fixed as (g,c) permutes G. Therefore

$$\begin{aligned} \phi_{\bar{k}[G]}^{G\times C}((g,c)) &= |\{h \in G : ghc = h\}| \\ &= |\{h \in G : c = h^{-1}g^{-1}h\}| \\ &= \begin{cases} |\mathrm{Cent}_G(c)| & \text{if } g^{-1} \text{ is } G\text{-conjugate to } c, \\ 0 & \text{otherwise,} \end{cases} \end{aligned}$$

where $\mathrm{Cent}_G(c)$ is the centralizer of c in G, whose cardinality was given as $\prod_{i:d|d_i} d_i$ in Theorem 15(iii). □

We next turn to computing the right side of (5.1). For this, we need some notation about the Brauer lifting process. Let μ be a subgroup of roots of unity inside $\bar{k}^\times$ that contains the eigenvalues of all p-regular elements of G, and fix an embedding $\mu \to \mathbb{C}^\times$. Call the image of an element of μ under this embedding its *lift*.

Assume that $g \in G = GL(V)$ is p-regular. Since g acts semisimply on V, it will have eigenvalues $\overline{\lambda}_1, \ldots, \overline{\lambda}_n$ in $\bar{k}^\times$ corresponding to a complete set of eigenvectors in $\overline{V}$. Denote the lifts of these eigenvalues $\lambda_1, \ldots, \lambda_n \in \mathbb{C}^\times$. Given c in G a regular element with a regular eigenvector having eigenvalue ζ, let $\omega \in \mathbb{C}^\times$ denote the lift of ζ.

Lemma 17. *With notation as above,*

$$\phi_{\bar{A}}^{G\times C}((g,c)) = \lim_{t\to\omega} \prod_{i=1}^{n} \frac{1-t^{d_i}}{1-\lambda_i t}, \tag{5.2}$$

Proof. This is essentially a calculation along the lines of Molien's Theorem [18, Proposition 4.3.1]. We start by computing the graded Brauer character for g on $\bar{S}$, which we identify with the symmetric algebra $\mathrm{Sym}(\overline{V})$. Note that the eigenvalues of g on $\mathrm{Sym}^m(\overline{V})$ will be all the monomials $\overline{\lambda}_1^{m_1}\cdots\overline{\lambda}_n^{m_n}$ with $\sum_i m_i = m$. Consequently,

$$\phi^G_{\mathrm{Sym}^m(V)}(g) = \sum_{\sum_i m_i = m} \lambda_1^{m_1}\cdots\lambda_n^{m_n}$$

$$\phi^G_{\mathrm{Sym}(V)}(g;t) = \prod_{i=1}^{n} \frac{1}{(1-\lambda_i t)}.$$

Since $\bar{S}^G = \bar{k}[f_1,\ldots,f_n]$ and f_i has degree d_i,

$$\phi^G_{\bar{S}^G}(g;t) = \mathrm{Hilb}(\bar{S}^G,t) = \prod_{i=0}^{n-1}\frac{1}{1-t^{d_i}}.$$

Let $g \in G$ be a p-regular element. Observe the following three facts

- $\mathrm{Sym}(\overline{V}) = \bar{k}[x_1,\ldots,x_n]$ is a free $\bar{S}^G$-module (see [18, Cor. 6.7.13]),
- $\bar{A}$ is a semisimple $\bar{k}[\langle g\rangle]$-module, and
- g acts trivially on $\bar{S}^G$.

From these three facts it follows that there is an isomorphism of graded $\bar{k}[\langle g\rangle]$-modules

$$\mathrm{Sym}(\overline{V}) \cong \bar{A}\otimes_{\bar{k}} \bar{S}^G.$$

This implies

$$\phi^G_{\mathrm{Sym}(\overline{V})}(g;t) = \phi^G_{\bar{A}}(g;t)\ \phi^G_{\bar{S}^G}(g;t).$$

Therefore

$$\phi^G_{\bar{A}}(g;t) = \frac{\phi^G_{\mathrm{Sym}(\overline{V})}(g;t)}{\phi^G_{\bar{S}^G}(g;t)} = \prod_{i=1}^{n}\frac{1-t^{d_i}}{1-\lambda_i t}. \tag{5.3}$$

To understand $\phi^{G\times C}_{\bar{A}}((g,c))$ from (5.3), note that c acts on the m^{th}-graded piece $\bar{A}_m$ by the scalar ζ^m. Hence $\phi^{G\times C}_{\bar{A}_m}((g,c))$ is ω^m times the coefficient of t^m in (5.3). Then $\phi^{G\times C}_{\bar{A}}(g,c)$ comes from summing this over all m, which is the same as setting $t=\omega$ in (5.3). □

Theorem 1 will now follow by comparing Proposition 16 with the following proposition.

Proposition 18. *Let c be a regular element in G of multiplicative order d, and let g be any element of G. Then*

$$\phi^{G\times C}_{\bar{A}}(g,c) = \begin{cases} \prod_{i:d|d_i} d_i & \text{if } g^{-1} \text{ is } G\text{-conjugate to } c,\\ 0 & \text{otherwise.}\end{cases}$$

Proof. Let ζ be the eigenvalue for c on a regular eigenvector v, and $\omega\in\mathbb{C}^\times$ its lift. The numerator of the rational function in (5.2) has $t=\omega$ as a root with multiplicity $a(d) = |\{i : d|d_i\}|$. Hence $\phi^{G\times C}_{\bar{A}}(g,c)$ will vanish unless the denominator also has $t=\omega$ as a root with this same multiplicity, that is, unless $\dim_{\bar{k}}\overline{V}(g,\zeta^{-1}) = a(d)$. By Theorem 15(iv), this requires g to be conjugate in G to c^{-1}.

When g is conjugate to c^{-1}, Theorem 15(v), implies that the eigenvalues of g lift to $\{\omega^{d_i-1}\}_{i=1}^n$. Hence

$$\begin{aligned}\phi_{\bar{A}}^{G\times C}(g,c) &= \lim_{t\to\omega}\prod_{i=1}^{n}\frac{1-t^{d_i}}{1-t\omega^{d_i-1}}\\ &= \prod_{i:d|d_i}\lim_{t\to\omega}\frac{1-t^{d_i}}{1-t\omega^{d_i-1}}\cdot\prod_{i:d\nmid d_i}\lim_{t\to\omega}\frac{1-t^{d_i}}{1-t\omega^{d_i-1}}\\ &= \prod_{i:d|d_i}\frac{-d_i\omega^{d_i-1}}{-\omega^{d_i-1}}\cdot\prod_{i:d\nmid d_i}\frac{1-\omega^{d_i}}{1-\omega\cdot\omega^{d_i-1}}\\ &= \prod_{i:d|d_i} d_i.\end{aligned}$$

□

6. Proof of Theorem 2

Proof for case (a). The result will follow from Theorem 1 when $|H|$ is invertible in $\bar{k}$. The fact that $\bar{A}$ and $\bar{k}[G]$ have the same $\bar{k}[G\times C]$-composition factors implies, by restriction, that they have the same $\bar{k}[H\times C]$-composition factors. Then they are isomorphic as $\bar{k}[H\times C]$-modules, because $|H\times C| = |H||C|$ is invertible in k, so the action is semisimple. Restricting to the H-invariant subspaces of each gives the desired isomorphism of $\bar{k}[C]$-modules, which is equivalent to the cyclic sieving phenomenon for $(X, X(t), C)$. □

Proof for case (b). Here we will show the rephrased version directly, using the same notation. Note $cgH = gH$ if and only if $g^{-1}cg$ lies in H, that is, if and only if c is conjugated by g into H. Proposition 10 and Theorem 15(iv) imply that there exists an element h in H conjugate in G to c if and only if $a_H(d) = a_G(d)$. When this occurs, by conjugation within G, we may assume without loss of generality that c lies in H. Applying Theorem 15(iii) to both G and H, it remains to show that

$$|\{gH \in G/H : g^{-1}cg \in H\}| = \frac{|\mathrm{Cent}_G(c)|}{|\mathrm{Cent}_H(c)|}. \tag{6.1}$$

Beginning with the left side of (6.1), one has

$$\begin{aligned}&|\{gH \in G/H : g^{-1}cg \in H\}|\\ &= \frac{1}{|H|}|\{g \in G : g^{-1}cg \in H\}|\\ &= \frac{1}{|H|}|\{h \in H : h \text{ is } G\text{-conjugate to } c\}|\cdot|\mathrm{Cent}_G(c)|\end{aligned}$$

Note that if h in H is G-conjugate to c, then

$$\dim_{\bar{k}} \overline{V}(h,\zeta) = a_G(d) = a_H(d)$$

and hence h is also *H-conjugate* to c by Theorem 15(iv). Thus the last expression above can be rewritten as

$$\frac{1}{|H|}|\{h \in H : h \text{ is } H\text{-conjugate to } c\}|\cdot|\mathrm{Cent}_G(c)| = \frac{|\mathrm{Cent}_G(c)|}{|\mathrm{Cent}_H(c)|},$$

as desired. □

7. The case of $G = GL_n(\mathbb{F}_q)$

In this section, we examine more closely the case $G = GL_n(\mathbb{F}_q)$.

The fact that

$$S^G = \mathbb{F}_q[D_{n,0}, D_{n,1}, \ldots, D_{n,n-1}]$$

is a polynomial algebra is a well-known result of Dickson [7]. The *Dickson polynomials* $D_{n,i}$ can be described explicitly, and $\deg(D_{n,i}) = q^n - q^i$; see [18, §8.1].

We begin by characterizing the regular elements in $GL_n(\mathbb{F}_q)$, and then study two interesting examples of subgroups H in G.

Theorem 19. *The following are equivalent for c in $G = GL_n(\mathbb{F}_q)$.*

(i) *c is regular.*
(ii) *The minimal polynomial for c is irreducible in $\mathbb{F}_q[x]$.*
(iii) *c coincides with one of the $\mathbb{F}_q$-linear maps that come from scalar multiplications by $\alpha \in \mathbb{F}_{q^n}^\times$, after identifying $\mathbb{F}_{q^n}$ with $(\mathbb{F}_q)^n$ as $\mathbb{F}_q$-vector spaces*[2]*.*

Proof. Note that the reflecting hyperplanes for $GL_n(\mathbb{F}_q)$ are exactly the zero sets of all (non-zero) linear forms $\ell(x)$ having $\mathbb{F}_q$-coefficients. Hence a vector $v \in \overline{V} = \overline{\mathbb{F}}_q^n$ is regular if and only if there is no such linear form vanishing on v, that is, if v lies in no proper subspaces defined over $\mathbb{F}_q$.

(i) implies (ii): When c is regular, it is semisimple (by Corollary 7), and hence its minimal polynomial $f(x)$ is a product of distinct irreducible factors. If there were more than one such factor of $f(x)$, then $\mathbb{F}_q^n$ would decompose into a nontrivial direct sum of proper c-stable $\mathbb{F}_q$-subspaces. Furthermore, after extending scalars, one of these subspaces will contain the regular eigenvector for c. But regularity implies that this eigenvector lies in no proper subspaces defined over $\mathbb{F}_q$.

(ii) implies (iii): When c has irreducible minimal polynomial $f(x)$ of degree d, its rational canonical form over $\mathbb{F}_q$, and hence its $GL_n(\mathbb{F}_q)$-conjugacy class, is completely determined by $f(x)$. Furthermore, this rational canonical form will coincide with that of scalar multiplication by any root α of $f(x)$ lying in the extension $\mathbb{F}_{q^d}$. Since the characteristic polynomial of c is a power of $f(x)$, one must have $d|n$, and hence $\alpha \in \mathbb{F}_{q^n}$.

(iii) implies (i): Given $\alpha \in \mathbb{F}_{q^n}^\times$, we must show that the $\mathbb{F}_q$-linear map c which is multiplication by α has a regular eigenvector. Since $\mathbb{F}_{q^n}^\times$ is cyclic, without loss of generality we may assume that α is a cyclic generator of $\mathbb{F}_{q^n}^\times$, so that α has minimal polynomial $f(x)$ over $\mathbb{F}_q$ which is irreducible of degree n. Then c acts in the $\mathbb{F}_q$-basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ for $\mathbb{F}_{q^n}$ by the companion matrix of $f(x)$, and hence has α as an eigenvalue, say with eigenvector v.

Let F denote both the Frobenius endomorphism on $\overline{\mathbb{F}}_q$, and also the endomorphism on $\overline{\mathbb{F}}_q^n$ that acts by F simultaneously in each component. Then

$$\alpha, F(\alpha), F^2(\alpha), \ldots, F^{n-1}(\alpha)$$

are the eigenvalues of c, which are all distinct by the separability of the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$. Their corresponding eigenvectors

$$v, F(v), F^2(v), \ldots, F^{n-1}(v)$$

[2]Such $\mathbb{F}_q$-linear maps are sometimes called *Singer cycles* in the case where α is a generator for the cyclic group $\mathbb{F}_{q^n}^\times$, and when one considers α as permuting the set of $\mathbb{F}_q$-lines in $\mathbb{F}_{q^n}$.

therefore form a $\overline{\mathbb{F}}_q$-basis for $\overline{\mathbb{F}}_q^n$. Thus v must be regular: if it were to lie in some proper subspace of $\overline{\mathbb{F}}_q^n$ defined over $\mathbb{F}_q$, the same would be true for all its Frobenius images $F^i(v)$, and they would not span $\mathbb{F}_q^n$. □

We next examine two interesting examples of families of subgroups H in $G = GL_n(\mathbb{F}_q)$. We should also mention that the original motivating example for Theorem 2(b) (and [13, Theorem 2]), namely the case where H is a *parabolic subgroup* of $G = GL_n(\mathbb{F}_q)$, is discussed already in [14, §9].

Example 20. An $\mathbb{F}_q$-*frame* in $\mathbb{F}_q^n$ is an unordered set $\{L_1, \ldots, L_n\}$ of lines (1-dimensional $\mathbb{F}_q$-subspaces) L_i giving rise to an $\mathbb{F}_q$-vector space decomposition $\mathbb{F}_q^n = \bigoplus_{i=1}^n L_i$. Let $H = \mathbb{F}_q^\times \wr \mathfrak{S}_n$ be the group of *monomial matrices* in $G = GL_n(\mathbb{F}_q)$, that is, the matrices with exactly one non-zero entry in each row and each column. Note that H is the (not-necessarily-pointwise) stabilizer of the particular $\mathbb{F}_q$-frame given by the coordinate axes in $\mathbb{F}_q^n$. Hence since G acts transitively on frames, the collection of cosets G/H is identified with the set X of all such frames.

Here S^H is a polynomial algebra, as it consists of the symmetric functions in the powers of the variables $x_1^{q-1}, \ldots, x_n^{q-1}$. Consequently,

$$X(t) := \frac{\mathrm{Hilb}(S^H, t)}{\mathrm{Hilb}(S^G, t)} = \frac{\prod_{i=0}^{n-1}(1 - t^{q^n - q^i})}{\prod_{i=1}^{n}(1 - t^{(q-1)i})}.$$

What does Theorem 2(b) tell us in this case? We demonstrate its utility by comparing calculations of the two sides of equation (2.5): the right side by a painless substitution of a root of unity, the left side by reasoning geometrically about the action of a regular element on frames.

By Theorem 19, a regular element in G corresponds to some $\alpha \in \mathbb{F}_{q^n}^\times$. Assume α has multiplicative order d. Assume the field extension $\mathbb{F}_q(\alpha)$ generated by α within $\mathbb{F}_{q^n}$ has $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^r}$, so that $r|n$, and r is the smallest positive integer for which $d|q^r - 1$.

Theorem 2(b)(rephrased) tells us that the number of $\mathbb{F}_q$-frames preserved under multiplication by α will be zero unless the two quantities

$$a_G(d) = \frac{n}{r} \quad \text{and} \quad a_H(d) = \frac{n}{d/\gcd(d, q-1)}$$

coincide. Thus there should be no $\mathbb{F}_q$-frames preserved by α unless $\frac{d}{\gcd(d,q-1)} = r$, in which case the right side of (2.5) tells us that the number of such frames should be

$$\frac{\prod_{\substack{0 \le i \le n-1 \\ i \equiv 0 \bmod r}} (q^n - q^i)}{\prod_{\substack{1 \le i \le n \\ i \equiv 0 \bmod r}} (q-1)i} = \frac{|GL_{\frac{n}{r}}(\mathbb{F}_{q^r})|}{(\frac{n}{r})!(q-1)^{\frac{n}{r}} r^{\frac{n}{r}}}. \tag{7.1}$$

To see how the left side of (2.5) gives an answer equivalent to (7.1), we must reason geometrically about how multiplication by α can preserve an $\mathbb{F}_q$-frame $\{L_1, \ldots, L_n\}$. This would require that α permutes the lines in the frame, and hence the set of lines decomposes into cycles $\mathcal{O}_1, \ldots, \mathcal{O}_m$ for this permutation. Each such cycle $\mathcal{O}_j$ must consist of exactly r of these $\mathbb{F}_q$-lines, because the $\mathbb{F}_q$-span of $\mathcal{O}_j$ must be an $\mathbb{F}_q(\alpha)(= F_{q^r})-$subspace of $\mathbb{F}_q(\alpha)$-dimension at most 1 (as it is $\mathbb{F}_q(\alpha)$-spanned by any line L_i in $\mathcal{O}_j$). Since each cardinality $|\mathcal{O}_j| = r$, one must have $m = \frac{n}{r}$. Also the cyclic subgroup $C = \langle \alpha \rangle$ of order d must have the C-stabilizer of any particular $\mathbb{F}_q$-line L_i in this frame of order $\frac{d}{r}$. On the other hand, this stabilizer subgroup

should be of order $\gcd(d, q-1)$, since it is the intersection of the cyclic groups C and $\mathbb{F}_q^\times$ inside the larger cyclic group $\mathbb{F}_{q^n}^\times$. Thus one recovers the requirement that $r = \frac{d}{\gcd(d,q-1)}$ in order for α to preserve any $\mathbb{F}_q$-frames at all.

If $r = \frac{d}{\gcd(d,q-1)}$, then the preceding discussion indicates how to parametrize all $\mathbb{F}_q$-frames in $\mathbb{F}_q^n$ preserved by α. To choose one, first choose an $\mathbb{F}_{q^r}$-frame in $\mathbb{F}_q^n$, and then within each of the $\mathbb{F}_{q^r}$-lines in this $\mathbb{F}_{q^r}$-frame, pick an $\mathbb{F}_q$-frame to be one of the sets $\mathcal{O}_j$. Because $r = \frac{d}{\gcd(d,q-1)}$, it follows that α will have every orbit of $\mathbb{F}_q$-lines of size r. Since each $\mathbb{F}_{q^r}$-line contains $[r]_q := \frac{q^r-1}{q-1}$ different $\mathbb{F}_q$-lines, there will be $\frac{[r]_q}{r}$ C-orbits from which to choose $\mathcal{O}_j$. Thus there are a total of

$$|\left\{\mathbb{F}_{q^r} - \text{frames in } \mathbb{F}_q^n\right\}| \cdot \left(\frac{[r]_q}{r}\right)^{\frac{n}{r}} = \frac{|GL_{\frac{n}{r}}(\mathbb{F}_{q^r})|}{\frac{n}{r}!(q^r-1)^{\frac{n}{r}}} \cdot \left(\frac{[r]_q}{r}\right)^{\frac{n}{r}}$$

choices, which agrees with (7.1).

The next example verifies directly a non-trivial instance of Conjecture 3.

Example 21. Let $G = GL_{2n}(\mathbb{F}_q)$ with q odd, and $H = Sp_{2n}(\mathbb{F}_q)$ the *symplectic group* that preserves some particular symplectic form on $\mathbb{F}_q^{2n}$. Since G acts transitively on symplectic forms, the collection of cosets G/H is identified with the set X of all symplectic forms.

The invariant ring S^H is *not* a polynomial algebra. Nevertheless, it was described by Carlisle and Kropholler (see [2, §8.3]). It is a complete intersection ring with the following presentation:

$$\mathbb{F}_q[\xi_1, \xi_2, \ldots, \xi_{2n-1}, D_{2n,n}, D_{2n,n+1}, \ldots, D_{2n,2n-1}]/(r_1, \ldots, r_{n-1})$$

where the $D_{2n,i}$ are the Dickson polynomials, ξ_i are homogeneous of degree $q^i + 1$, and r_i is a homogeneous relation of degree $q^{2n} + q^i$. Consequently, S^H is a Cohen-Macaulay ring with Hilbert series

$$\mathrm{Hilb}(S^H, t) = \frac{\prod_{i=1}^{n-1}(1 - t^{q^{2n}+q^i})}{\prod_{i=n}^{2n-1}(1 - t^{q^{2n}-q^i})\prod_{i=1}^{2n-1}(1 - t^{q^i+1})}$$

and

$$X(t) := \frac{\mathrm{Hilb}(S^H, t)}{\mathrm{Hilb}(S^G, t)} = \frac{\prod_{i=1}^{n-1}(1 - t^{q^{2n}+q^i})\prod_{i=0}^{n-1}(1 - t^{q^{2n}-q^i})}{\prod_{i=1}^{2n-1}(1 - t^{q^i+1})}.$$

This gives an opportunity to verify directly Conjecture 3, (the cyclic sieving phenomenon) for this particular G and H. For any regular element c in G, we must compare the number of symplectic forms fixed by c with the substitution $X(\omega)$, where ω is a complex root of unity of the same multiplicative order as c.

Again by Theorem 19, a regular element in G corresponds to some α in $\mathbb{F}_{q^{2n}}^\times$, say of multiplicative order d. Assume α generates the extension $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^r}$ inside $\mathbb{F}_{q^{2n}}$, so that $r|2n$, and r is the smallest positive integer for which $d|q^r - 1$.

Let ω in $\mathbb{C}^\times$ be a primitive d^{th} root of unity. We begin by computing $X(\omega)$. The numerator of $X(t)$ has $t = \omega$ as a zero of order at least $\frac{2n}{r} \geq 1$, due to its factors of the form $1 - t^{q^{2n}-q^{ri}}$. Hence $X(\omega) = 0$ unless $t = \omega$ is a root of the denominator, that is, unless $d|q^i + 1$ for some i. Let i_0 be the smallest positive integer for which $d|q^{i_0} + 1$. Since $d|q^r - 1$, one can check that $d|q^j + 1$ if and only if $j \equiv i_0 \mod r$. Thus we may assume i_0 lies in the range $[1, r]$. Furthermore, the fact that d divides

both $q^r - 1$ and $q^{i_0} + 1$ forces d to divide $q^r + q^{i_0} = q^{i_0}(q^{r-i_0} + 1)$. Hence $d | q^{r-i_0} + 1$ because $\gcd(d, q^{i_0}) = 1$. Thus either

- $i_0 = r$, and $d | q^{r-i_0} + 1 = 2$, so that $d = 1$ or $d = 2$, or
- $i_0 = r - i_0$, so that $r \geq 2$ is even and $i_0 = \frac{r}{2}$.

In the former case where $d = 1$ or 2, one has $\omega = +1, -1$, and one can see that $X(1) = X(-1) = [G : H]$ (using the fact that q is odd).

In the latter case where $r \geq 2$ is even and $i_0 = \frac{r}{2}$, one calculates that

$$\begin{aligned} \lim_{t \to \omega} X(t) &= \frac{\prod_{\substack{1 \leq i \leq n-1 \\ i \equiv \frac{r}{2} \bmod r}} (q^{2n} + q^i) \prod_{\substack{0 \leq i \leq n-1 \\ i \equiv 0 \bmod r}} (q^{2n} - q^i)}{\prod_{\substack{1 \leq i \leq 2n-1 \\ i \equiv \frac{r}{2} \bmod r}} (q^i + 1)} \\ &= \frac{\prod_{j=0}^{\lfloor \frac{m}{2} \rfloor - 1} (Q^{2m} + Q^{2j+1}) \prod_{j=0}^{\lceil \frac{m}{2} \rceil - 1} (Q^{2m} - Q^{2j})}{\prod_{j=0}^{m-1} (Q^{2j+1} + 1)} \\ &= Q^{\binom{m}{2}} (Q-1)(Q^2+1)(Q^3-1)(Q^4+1) \cdots (Q^m + (-1)^m) \end{aligned} \tag{7.2}$$

where $Q := q^{i_0} = q^{\frac{r}{2}}$ and $m := \frac{2n}{r}$. Denote the last quantity appearing in (7.2) by $f_m(Q)$.

Summarizing these calculations, we have

$$X(\omega) = \begin{cases} [G : H] (= |X|) & \text{if } d = 1, 2, \\ f_{\frac{2n}{r}}(Q) & \text{if } r \text{ is even}, \\ 0 & \text{otherwise.} \end{cases} \tag{7.3}$$

Thus to verify the cyclic sieving phenomenon, it remains to check that the right-hand side of (7.3) coincides with the number of symplectic forms on $\mathbb{F}_q^{2n}$ fixed under multiplication by α, that is, satisfying

$$\langle \alpha x, \alpha y \rangle = \langle x, y \rangle. \tag{7.4}$$

To this end, consider the $\mathbb{F}_q$-linear map c on $\mathbb{F}_{q^{2n}}$ which is multiplication by α. Its eigenvalues are $\alpha, F(\alpha), \ldots, F^{2n-1}(\alpha)$, where F denotes the Frobenius endomorphism on $\mathbb{F}_{q^{2n}}$. Since $\alpha \in \mathbb{F}_{q^r}$, one has $F^r(\alpha) = \alpha$ and if one extends the scalars to $\mathbb{F}_{q^r}$, there will be an α-eigenspace for c which is $\frac{2n}{r}$-dimensional with basis $v_1, \ldots, v_{\frac{2n}{r}}$ in $\mathbb{F}_{q^r}^{2n}$. The remaining eigenvectors for c are the images $F^j(v_i)$ under powers of the Frobenius map F.

How can an $\mathbb{F}_q$-bilinear symplectic form $\langle \cdot, \cdot \rangle$ on $\mathbb{F}_q^{2n}$ be preserved by α? Extending it to an $\mathbb{F}_{q^r}$-bilinear symplectic form on $\mathbb{F}_{q^r}^{2n}$, one notes that it will have the following invariance with respect to the Frobenius map F:

$$\langle F(x), F(y) \rangle = F(\langle x, y \rangle) \tag{7.5}$$

Furthermore, if w_1, w_2 are c-eigenvectors in $\mathbb{F}_{q^r}^{2n}$ with eigenvalues λ_1, λ_2 in $\mathbb{F}_{q^r}$, then (7.4) forces

$$\langle w_1, w_2 \rangle = \langle c(w_1), c(w_2) \rangle = \lambda_1 \lambda_2 \langle w_1, w_2 \rangle \tag{7.6}$$

so that either $\lambda_2 = \lambda_1^{-1}$ or $\langle w_1, w_2 \rangle = 0$. Thus nondegeneracy of the symplectic form implies that the eigenvalues of c are closed under taking reciprocals. There are two ways this can happen.

If $r = 1$, so that $\alpha \in \mathbb{F}_q$, then α must be self-reciprocal. Thus $\alpha = \pm 1$, so $d = 1$ or 2. In this case, α preserves every symplectic form, in agreement with the right side of (7.3).

If $r > 1$, then $F^{i_0}(\alpha) = \alpha^{-1}$ for some smallest positive integer i_0. This means $\alpha^{q^{i_0}+1} = 1$ or $d|q^{i_0} + 1$, forcing $r = 2i_0$ to be even (again in agreement with the right side of (7.3)). In this case, (7.5) and (7.6) imply that the symplectic form is completely determined by a choice of the matrix of values $a_{ij} = \langle v_i, F^{\frac{r}{2}}(v_j)\rangle$ for $i, j = 1, \ldots, \frac{2n}{r}$. Furthermore, note that

$$a_{ji} = \langle v_j, F^{\frac{r}{2}}(v_i)\rangle = \langle F^{\frac{r}{2}}F^{\frac{r}{2}}v_j, F^{\frac{r}{2}}(v_i)\rangle = F^{\frac{r}{2}}(\langle F^{\frac{r}{2}}v_j, v_i\rangle) = -F^{\frac{r}{2}}(a_{ij}).$$

Thus a_{ij} is *skew-Hermitian* of size $\frac{2n}{r}$ with entries in $\mathbb{F}_{Q^2}$, where $Q := q^{\frac{r}{2}}$ and $F^{\frac{r}{2}}$ is the conjugation that generates the Galois group of $\mathbb{F}_{Q^2}/\mathbb{F}_Q$. Nondegeneracy of the symplectic form forces (a_{ij}) to be nonsingular, and it is not hard to check that the converse holds: every such nonsingular skew-Hermitian matrix of size $\frac{2n}{r}$ over $\mathbb{F}_{Q^2}$ gives rise to a symplectic form on $\mathbb{F}_{q^r}^{2n}$ which is the extension of a symplectic form on $\mathbb{F}_q^{2n}$ invariant under multipication by α.

It remains to show that the previously defined function $f_m(Q)$ counts nonsingular skew-Hermitian matrices of size m over $\mathbb{F}_{Q^2}$. It is known [4, Theorem 3, (4.4)] that $f_m(Q)$ counts nonsingular *Hermitian* matrices of size m over $\mathbb{F}_{Q^2}$. On the other hand, multiplication by any scalar $\beta \in \mathbb{F}_{Q^2}$ which satisfies $F^{\frac{r}{2}}(\beta) = -\beta$ (that is, β is a root of $x^{q-1} + 1 = 0$) gives a rank-preserving bijection between Hermitian and skew-Hermitian matrices.

8. Filtrations of projective modules

In this section we explore further the relationship between the module structure of the coinvariant algebra and the regular representation.

Proposition 22. *Let G be a finite subgroup of $GL(V)$ for which S^G is polynomial, and let C be the cyclic subgroup generated by a regular element c in G. Let $d = |C|$ be the order of c.*

Then for each integer n, the direct sum

$$\bigoplus_{m \,\equiv\, n \bmod d} \bar{A}_m \tag{8.1}$$

has the same composition factors as a projective $\bar{k}[G]$-module.

Proof. The regular element c acts on the m^{th} homogeneous component $\bar{A}_m$ by the scalar ζ^m. Thus the direct sum (8.1) is the ζ^n-eigenspace of c acting on $\bar{A}$. By Theorem 1 this direct sum has the same $\bar{k}[G]$-module composition factors as the ζ^n-eigenspace of c acting on $\bar{k}[G]$.

The group algebra $\bar{k}[C]$ contains d primitive orthogonal idempotents $e_0, \ldots, e_{d-1}$ so that for any right $\bar{k}[C]$-module M the subspace Me_i is the ζ^i-eigenspace of c. We have $\bar{k}[G] = \bar{k}[G]e_0 \oplus \cdots \oplus \bar{k}[G]e_{d-1}$, and these summands of the regular representation are projective modules for $\bar{k}[G]$. The result follows. □

We illustrate Proposition 22 by means of an example. Let $G = S_4$ be the symmetric group of degree 4, acting on a 4-dimensional vector space V with basis v_1, v_2, v_3, v_4 by permuting the basis vectors in the faithful permutation representation. In all characteristics the invariants S^G are a polynomial ring on the elementary

symmetric polynomials in degrees 1, 2, 3 and 4. According to Springer [19] the regular elements when k has characteristic zero are the powers of 3-cycles or 4-cycles. We next work out explicitly the regular elements in S_4 when k has characteristic 2 or 3.

When k has characteristic 2, regular elements must have order prime to 2 (by Corollary 7) so 3-cycles are the only possibility. The eigenvector $v_1 + \zeta v_2 + \zeta^2 v_3$ of the 3-cycle $(1, 2, 3)$ (where ζ is a primitive cube root of 1) does not lie in any reflecting hyperplane, and from this we see that $(1, 2, 3)$ and the other 3-cycles are indeed regular.

Similarly in characteristic 3 we see that any regular element must be a 4-cycle or the square of a 4-cycle. If ζ is a primitive fourth root of 1 then $v_1+\zeta v_2+\zeta^2 v_3+\zeta^3 v_4$ is an eigenvector of $(1, 2, 3, 4)$ which does not lie in any reflecting hyperplane and we see from this that the 4-cycles are indeed regular in characteristic 3. In fact the squares of 4-cycles are also regular in characteristic 3, but we will not mention them further since the sieving phenomenon they provide is deducible from that of the 4-cycles.

We claim that in characteristic 2 the module structures of the homogeneous components of A are given by

Degree	0	1	2	3	4	5	6
Module Structure	1	$\begin{smallmatrix}1\\2\end{smallmatrix}$	$\begin{smallmatrix}1\oplus 2\\2\end{smallmatrix}$	$\begin{smallmatrix}1\\2\end{smallmatrix} \oplus \begin{smallmatrix}2\\1\end{smallmatrix}$	$\begin{smallmatrix}2\\1\oplus 2\end{smallmatrix}$	$\begin{smallmatrix}2\\1\end{smallmatrix}$	1

and in characteristic 3 they are

Degree	0	1	2	3	4	5	6
Module Structure	1	3	$\begin{smallmatrix}1\\-1\end{smallmatrix} \oplus 3$	$3 \oplus -3$	$\begin{smallmatrix}1\\-1\end{smallmatrix} \oplus -3$	-3	-1

In characteristic 2, S_4 has two simple modules, of dimensions 1 and 2, and we denote these modules by their dimensions. In characteristic 3, S_4 has 4 simple modules which we denote $1, -1, 3, -3$. These are, respectively, the trivial module, the sign representation, the 3-dimensional module which is a direct summand of V^*, and $3 \otimes -1$. These latter 3-dimensional modules are projective and injective (they are blocks of defect zero) and appear as direct summands of any module of which they are a composition factor. In these tables we indicate a module by presenting its composition factors in certain positions relative to one another. Where a module is the direct sum of two submodules this is indicated with a $\oplus$ sign. Where a module is a non-split extension of one module by another, this fact is indicated by writing the submodule underneath the factor module.

It is well-known that the indecomposable projective S_4-modules in characteristic 2 have the structure

$$\begin{smallmatrix}&1&\\2&\oplus&1\\&1&\end{smallmatrix}\,, \qquad \begin{smallmatrix}2\\2\oplus 1\\2\end{smallmatrix}$$

and in characteristic 3 they are

$$\begin{smallmatrix}1\\-1\\1\end{smallmatrix}\,, \quad \begin{smallmatrix}-1\\1\\-1\end{smallmatrix}\,, \quad 3, \quad -3.$$

We refer here to [1] for such calculations. We see in our example that in characteristic 2 the composition factors of A in degrees which form a residue class modulo 3 are always the composition factors of a projective module, as predicted by Proposition 22. To be explicit, these residue classes of degrees are $\{0, 3, 6\}$, $\{1, 4\}$ and $\{2, 5\}$ and in each case the composition factors of A in these degrees are the composition factors of an indecomposable projective module. In characteristic 3 the composition factors which occur in degrees $\{0, 4\}$, $\{1, 5\}$, $\{2, 6\}$ and $\{3\}$ (these being the residue classes modulo 4, the order of a regular element) are in each case also composition factors of a projective module.

More than this is true for this example. In each characteristic, and for each of these residue classes of degrees, there is a filtration of a projective module such that the factors in the filtration taken in ascending order are isomorphic to the homogeneous terms of A with degrees in that residue class, taken in ascending order. Such calculations suggest the following question.

Question 23. Let G be a finite subgroup of $GL(V)$ for which S^G is polynomial and let C be the subgroup generated by a regular element in G.

Does there always exist a filtration of $\bar{k}[G]$ by $\bar{k}[G \times C]$-modules so that the factors, taken in ascending order, are isomorphic as $\bar{k}[G \times C]$-modules to the homogeneous terms of $\bar{A}$, taken in ascending order of degree?

An affirmative answer would imply that each eigenspace of C in its action on $\bar{k}[G]$ has a filtration whose factors are the terms of $\bar{A}$ in a residue class modulo $|C|$, which is the phenomenon we have been observing. We have been able to answer in the affirmative a weaker question, in which only the action of $\bar{k}[G]$ is considered, but have been unable to extend this to an action of $\bar{k}[G \times C]$.

We conclude by explaining how the above tables may be obtained. It is comparatively easy to obtain the multiplicities of the composition factors, and this may be done in several ways. One way is to compute for each simple module U the generating function of composition factor multiplicities

$$P_U(S, t) = \sum_{n=0}^{\infty} [\mathrm{Sym}^n(V) : U]\, t^n$$

of the homogeneous terms of $S = \mathrm{Sym}(V)$ using Molien's theorem [18]. Here $[\mathrm{Sym}^n(V) : U]$ denotes the composition factor multiplicity of U in $\mathrm{Sym}^n(V)$. We now use Mitchell's observation [12, Proposition 1.3] which implies that

$$P_U(S, t) = P_U(A, t)\, \mathrm{Hilb}(S^G, t).$$

Computing the precise module structure of the terms in the coinvariant algebra is more delicate. We may exploit the fact that it is a Poincaré duality algebra [18], so that in this case $A_n \cong (A_{6-n})^* \otimes A_6$. This means that we only need determine the module structure up to degree 3.

In characteristic 2 the permutation module V has the structure $\begin{smallmatrix} 1 \\ 2 \\ 1 \end{smallmatrix}$, which we may confirm by Brauer characters and Frobenius reciprocity (the adjoint property of induction and restriction) to show that the module has no 2-dimensional submodule or quotient. Factoring out the invariants gives $\begin{smallmatrix} 1 \\ 2 \end{smallmatrix}$ as claimed. In degree 2 one may employ similar but more elaborate arguments, but in degree 3 the determination of the module structure was ultimately done by computer calculation using software written in the package GAP. This can also be used to handle the degree 2 case.

In characteristic 3 the composition factors 3 and -3 which occur are all projective and so appear as direct summands. The only question is to determine whether or not the 1 and -1 composition factors occur in a non-split extension. From knowledge of the projective modules we see that there is no non-split extension of 1 by itself in characteristic 3, and that if the degree 2 module of A were semisimple it would imply that the polynomial ring has more invariants in degree 2 than it actually has.

9. Acknowledgments

The authors thank J. Hartmann, G. Kemper, W. Messing, A. Shepler, and L. Smith for helpful comments.

References

[1] D. Benson, Modular Representation Theory: New Trends and Methods, Lecture Notes in Math. 1081, Springer-Verlag 1984
[2] D. Benson, Polynomial invariants of finite groups. *London Math. Society Lecture Notes* **190**, Cambridge Univ. Press, 1993.
[3] N. Bourbaki, Lie groups and Lie algebras. Chapters 4–6. Translated from the 1968 French original by Andrew Pressley. Elements of Mathematics. Springer-Verlag, Berlin, 2002
[4] L. Carlitz and J. Hodges, Representations by Hermitian forms in a finite field. *Duke Math. J.* **22** (1955), 393–405.
[5] C. Chevalley, Invariants of finite groups generated by reflections. *Amer. J. Math.* **77** (1955), 778–782.
[6] C.W. Curtis and I. Reiner, Representation theory of finite groups and associative algebras. Pure and Applied Mathematics, Vol. XI, Wiley Interscience Publishers, New York, 1962.
[7] L.E. Dickson, A fundamental system of invariants of the general modular linear group with a solution of the form problem. *Trans. Amer. Math. Soc.* **12** (1911), 75–98.
[8] J. Hartmann and A.V. Shepler, Jacobian of reflection groups, ArXiv preprint `math.RT/0405135`.
[9] T.J. Hewett, Modular invariant theory of parabolic subgroups of $\mathrm{GL}_n(F_q)$ and the associated Steenrod modules. *Duke Math. J.* **82** (1996), 91–102.
[10] N.J. Kuhn and S.A. Mitchell, The multiplicity of the Steinberg representation of $\mathrm{GL}_n F_q$ in the symmetric algebra. *Proc. Amer. Math. Soc.* **96** (1986), 1–6.
[11] W. Kraśkiewicz and J. Weyman, Algebra of coinvariants and the action of a Coxeter element. *Bayreuth Math. Schr.* **63** (2001), 265–284.
[12] S.A. Mitchell, Finite complexes with $A(n)$-free cohomology. *Topology* **24** (1985), 227–246.
[13] V. Reiner, D. Stanton, and P. Webb, Springer's theorem for modular coinvariants of $GL_n(\mathbb{F}_q)$, unpublished manuscript, June 2003. Available at `www.math.umn.edu/~reiner`.
[14] V. Reiner, D. Stanton, and D. White, The cyclic sieving phenomenon, J. Combin. Theory Ser. A **108** (2004), 17 – 50.
[15] A. Grothendieck, Séminaire de géométrie algébriques du Bois Marie(SGA 1), Revêtements étale et groupes fôndamentales.
[16] J.-P. Serre, Groupes finis d'automorphismes d'anneaux locaux réguliers, Colloque d'Algébre ENSJF (Paris, 1967), pp. 8-01–8-11
[17] G.C. Shephard and J.A. Todd, Finite unitary reflection groups. *Canadian J. Math.* **6** (1954), 274–304.
[18] L. Smith, Polynomial invariants of finite groups. *Research Notes in Mathematics* **6**, A K Peters, Ltd., Wellesley, MA, 1995.
[19] T.A. Springer, Regular elements of finite reflection groups. *Invent. Math.* **25** (1974), 159–198.
[20] J. Stembridge, On the eigenvalues of representations of reflection groups and wreath products, *Pac. J. Math.* **140** (1989), 353–396.

E-mail address: `(reiner,stanton,webb)@math.umn.edu`

School of Mathematics, University of Minnesota, Minneapolis, MN 55455, USA